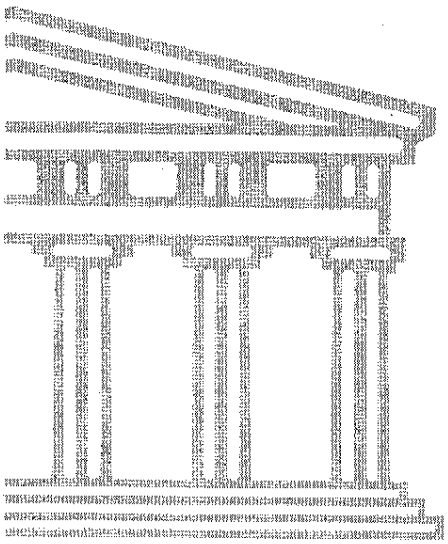

UNIVERSITY OF WESTERN CAPE (UWC)

NETWORK SECURITY POLICY

DATE OF LAST APPROVAL: C2004/5

UNIVERSITY of the WESTERN CAPE

A place of quality, a place to grow, from hope to action through knowledge

Network Security Policy

University of the Western Cape Policy *ICS/2004.02*

Background

The University of the Western Cape (UWC) provides network services to a large number and variety of users, including staff, students and external constituencies. Compromised security for any networked system can have a detrimental impact on other networked systems and even bring down the entire campus network. Information and Communication Services (ICS) is the primary information-technology provider on UWC's campus, with services for telephony, computing, and networking. ICS has campus-wide responsibility to maintain the integrity and security of networked systems and to provide the wiring and cabling infrastructures that support voice, data and video services.

This policy encompasses all systems directly connected to the UWC networks and systems on satellite networks that receive network service from the campus backbone. This includes campus Internet connections, 10BaseT, 100BaseT 1000BaseT, subscriber lines and Wireless Networks.

Policy

1. Network Traffic

!CS will control access to all intra-campus traffic, all inbound and outbound Internet traffic. The ICS Executive Director or his/her designee will determine what Internet traffic will be permitted. The Information Systems Committee (CISC) will provide oversight to ensure that the traffic limitations are consistent with both the business and academic goals of UWC.

2. Network Servers

All Network Servers must be registered through ICS to ensure that any additions or changes to the Network Servers will not have adverse effects on the network or attached resources.

3. Network Management

3.1. ICS or and JCS designee is authorized to perform a security audit of any UWC network device at any time.

3.2. JCS is the primary administrative contact for all network security related activities.

3.3. ICS will prepare recommendations and guidelines for network and system administrators and will post them on the JCS web pages. JCS will publish security alerts, vulnerability notices and patches, and other pertinent information in an effort to prevent security breaches.

3.4 JCS will coordinate investigations into any alleged computer or network security compromises, incidents, and/or problems. To ensure that this coordination is effective, ICS requests that security compromises be reported (Ext 2000 or e-mail: helpdesk@uwc.ac.za).

3.5. ICS will monitor backbone network traffic in real-time to detect unauthorized activity or intrusion attempts.

3.6. If scans or network monitoring identifies security vulnerabilities, the cooperation of the system owners and system managers for the systems and the networks will be required. If the appropriate contact cannot be determined, the department's management will be notified. When a security problem (or potential security problem) is identified JCS will take steps to disable network access to those systems and/or devices until the problems have been rectified.

3.7. In line with this, ICS has the right to remove any network segment from the campus network until problems affecting the network are identified and solved.

Procedures and Guidelines

All network users are responsible for understanding this policy and its implications. To obtain more information regarding network security, users may contact ICS by phoning 2000 or e-mailing: helpdesk(w,uwc.ac.za.

Responsible Organization

The Office of the Executive Director for Information and Communication Services will be responsible for this policy and for any appeals of JCS decisions relating to the network security. This policy will be reviewed yearly by ICS, and changes will be authorized by the approval of the Information Systems Committee (CISC). JCS will review network security best practices on an annual basis and recommend changes to this policy as needed.

Approved by Council on 4 December 2004 (C2004/5)